December 2012
GFK-1085X

IMPORTANT PRODUCT INFORMATION

READ THIS INFORMATION FIRST

Product: Factory LAN TCP/IP Ethernet Interface Module for Series 90-30 PLC
IC693CMM321-KN with Firmware Release 3.20

Ethernet Firmware version 3.20 addresses product security issues identified in Security Advisory document KB15240 (http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15240). GE Intelligent Platforms strongly recommends that you update to firmware version 3.20 to protect your system from these issues.

Important Note: Until the Station Manager password has been changed to a value other than "system," the password vulnerabilities will remain exploitable via the serial Station Manager and all access to Modify-level commands will be disabled on the Ethernet remote Station Manager.

This module provides MODBUS/TCP Master and Slave functionality. It provides network communications using the SRTP (Service Request Transfer Protocol) over standard TCP/IP (Transmission Control Protocol / Internet Protocol) on an Ethernet Local Area Network (LAN). The Ethernet Interface supports communication between Series 90 PLCs and PACSystems Rx7i controllers equipped with TCP/IP Ethernet Interfaces, and VersaMax PLCs equipped with EBI001 modules.

Documentation

For changes and additions to user documentation, see page 8.

TCP/IP Ethernet Communications User's Manual, GFK-1541 version B or later

TCP/IP Ethernet Communications Station Manager Manual, GFK-1186 version G or later

Release History

Part Number	*Firmware Version*	*Date*	*Comments*
IC693CMM321-KN	3.20	Dec. 2012	Addresses product security issues identified in Security Advisory document KB15240 (http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15240).
IC693CMM321-KM	3.14	Oct. 2010	Resolves intermittent failure of Modbus/TCP port to respond to Modbus/TCP Client requests.
IC693CMM321-KL	3.13	Mar. 2010	Hardware update to remove AAUI port.
IC693CMM321-JL	3.13	Nov. 2009	See GFK-1085U for problem resolved.
IC693CMM321-JK	3.12	Jan. 2008	See GFK-1085T for problem resolved.
IC693CMM321-HJ	3.11	Jan. 2005	See GFK-1085S for problems resolved.
IC693CMM321-GH	3.10	Mar. 2003	Adds MODBUS/TCP COMMREQ operations for Master and Slave; Corrects problem with interruption of Ethernet transmission.
IC693CMM321-GH	3.10	Jul. 2002	MODBUS/TCP Master and Slave functionality for modules with catalog numbers IC693CMM321-Fx.
IC693CMM321-FG	3.00	Nov. 2001	Full duplex capability; 10Base-T port.
IC693CMM321-EF	2.20	Nov. 1999	See GFK-1085L for new features and problems resolved.
IC693CMM321-EE	2.10	Jul. 1997	See GFK-1085K for new features and problems resolved.
IC693CMM321-DD	2.00	Dec. 1996	Hardware change.
IC693CMM321-CD	2.00	Oct. 1996	Adds support for Unsolicited Messages.
IC693CMM321-CC	1.11	Jun. 1996	See GFK-1085E for new features and problems resolved.
IC693CMM321-AA/BA	1.00	Dec. 1995	Initial release. Version –BA adds CE Mark approval.

Release 3.20 Details

Firmware Updates

- Firmware releases numbered 3.00 and greater apply only to modules with hardware version -Fx or later. Users of IC693CMM321-Ex and earlier modules can update by replacing their older Ethernet Interface module with a later module.
- Hardware versions –Fx and later can be upgraded to hardware version -Kx by returning the module to the factory.

Firmware Field Upgrade Kit

The following field upgrade kit for firmware version 3.20 can be downloaded from the Support website at http://support.ge-ip.com.

44A751570-G06

A Station Manager cable (IC693CBL316) is required to update the firmware.

Caution

***Do not* attempt to upgrade your IC693CMM321 to release 3.14 or later unless your Series 90-30 PLC has a reliable power source. DO NOT turn power off during the upgrade process.**

Functional Compatibility

Firmware release 3.20 of the IC693CMM321 is compatible with these products:

- Series 90-30 PLC CPU firmware version 6.50 or later; restricted operation with CPU firmware 5.03 (6.03 for Model 351 CPU). See “Additional Restrictions with CPU Firmware Earlier than Version 6.50” on page 3.
- PLC Logic Developer version 2.11 or later.
- VersaPro version 1.01 or later. Version 2.02 or later is required to store hardware configurations that contain module initialization files larger than 32,768 bytes.
- Control programming software, version 2.01 or later.
- Logicmaster 90-30 programming software IC693 version 6.01 or later.
- Logicmaster 90-30 TCP/IP Ethernet. Version 7.01 or later is required for Ethernet communication with the PLC.

Problems Resolved by Firmware Release 3.20

Addresses product security issues

Firmware version 3.20 addresses product security issues identified as Security Advisory GEIP12-18 in Security Advisory document KB15240 (http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15240).

Restrictions and Open Issues

- The Ethernet Interface sometimes generates multiple exception log events and PLC Fault Table entries when a single error condition occurs. Under repetitive error conditions, the exception log and/or PLC Fault Table can be completely filled with repetitive error messages.
- Initialization errors that generate any of the following exception log events should also restart the Ethernet Interface into Maintenance state: event 1b, entry 2 = 0003h, event 1c, entry 2 = 25h, or event 1c, entry 2 = 26h. The Ethernet Interface does not restart in these conditions.
- Use of the same IP Address by this Ethernet Interface and by another device on the same network results in the PLC Fault Table message "Bad remote application request; discarded request." This condition should be identified more precisely.
- When the client or server PLC scan time exceeds 100 ms, channels may fail with error codes 2411, 0B11, 9B90, 3F11, or 9590. The error codes may be viewed by doing a Stat H command.
- While a local Station Manager "TRACE LZ" troubleshooting command is in effect at an Ethernet Interface, do not issue Station Manager "REM <node> TEST" commands to it from a remote Interface. Doing so can cause errant behavior, including Interface lockup and loss-of-module in the PLC fault table.
- After performing a firmware update to an Ethernet Interface in which one or more Advanced User Parameters have been set to non-default values, the PLC Fault Table does not contain the message it should ("LAN IF can't init-check parms; running soft Sw Utl"); rather, no fault table entry appears. There is no indication in the fault table that the Ethernet Interface has entered Maintenance state to permit resetting of the user parameter(s). The Ethernet Interface does generate an entry in its exception log.
- The TCP tallies CurEstab and EstabRes do not always report the correct value.
- An Information Report channel may remain in the AWAIT_DRSP or AWAIT_CRSP state indefinitely if the remote host fails to send a response.
- When using VersaPro via Ethernet through this Ethernet Interface, a Clear operation that does not include clear of Software Configuration causes VersaPro to stop responding. This behavior is not observed using the other Ethernet programmers or if VersaPro is connected to the PLC via the Ethernet Interface within an IC693CPU364. Rebooting the VersaPro host PC is often required to re-establish communication with the PLC.

Additional Restrictions with CPU Firmware Earlier Than Version 6.50

Ethernet Programming Not Supported

Using a PLC programmer via Ethernet requires IC693 CPU version 6.5 or later. The programmer may appear to connect with a PLC using older CPU firmware, but essential functions will not work correctly.

CAUTION

Do not attempt to use an Ethernet programmer with CPU firmware earlier than version 6.50. Unpredictable operation of the PLC CPU and MS-DOS programming software will occur.

Single Incoming Network Connection to CPU

PLC CPU firmware versions earlier than 6.50 can support only one incoming network connection through the Ethernet Interface at a time. The Ethernet Interface consequently supports only one incoming connection at a time when used with this CPU firmware.

No Operation in Expansion or Remote Rack

With CPU firmware versions earlier than 6.50, locate the Ethernet Interface in the main PLC rack only (Rack 0, which contains the CPU). The Ethernet Interface is not supported by this CPU firmware in an expansion or remote PLC rack.

Incoming Network Connection May Be Refused After Restart

After any restart, including power up, the Ethernet Interface is unable to accept incoming network connections for approximately 2.5 seconds after the LAN Interface OK bit of the LAN Interface Status Word is set. This occurs only with CPU firmware earlier than version 6.50.

Unconfigured Ethernet Interface Inoperative for Two Minutes After Restart

With CPU firmware versions earlier than 6.50, an unconfigured Ethernet Interface waits for two minutes after each restart to receive valid configuration data from the PLC CPU. The interface slowly flashes its Module OK LED and is not operational during this time. This behavior occurs when a new interface is powered on for the first time. It also occurs when a PLC Programmer user clears the PLC configuration, or stores a new configuration with an empty slot or different module type at the location where the Ethernet Interface is installed.

Operational Notes

Remote Station Manager access is disabled until the Station manager password is changed

GE Intelligent Platforms strongly recommends that you change the Station Manager password to a value other than the default. Until the Station Manager password has been changed to a value other than “system”, the password vulnerabilities will remain exploitable via the serial Station Manager and all access to Modify-level commands will be disabled on the Ethernet remote Station Manager.

Modbus/TCP or SRTP connections get closed after inactivity of 7 minutes or more

After establishing Modbus/TCP or SRTP connection, if there is no communication activity on the connection for 7 minutes or more, the idle timer will expire and the TCP connection will be closed.

Power Loss During Field Upgrade Newer May Leave Ethernet Module Inoperative

The field upgrade kit for release 3.14 (including ZIP files downloaded from the Technical Support Web site) replaces the software loader of the IC693CMM321, as well as the TCP/IP software, when the module contains firmware version 3.10 or older before the upgrade. A power interruption during the approximately three seconds required to re-program flash memory with the new software loader will cause the module to become completely inoperative. To recover from this condition, the module must be returned to the factory.

CAUTION

DO NOT attempt to upgrade your IC693CMM321 to release 3.14 from release 3.10 or older unless your Series 90-30 PLC has a reliable power source.
DO NOT turn power off during the upgrade process.

This Firmware Release is Incompatible with Version IC693CMM321-Ex or Older Hardware

You should not attempt to use this firmware with older versions of this module. If this firmware version were to be loaded to an IC693CMM321-Ex or older version of this module, the module would not function as expected, and the following symptoms would be observed:

1. The interface is unable to go online.
2. The STAT and SER LEDs blink alternately at a ½-second rate.
3. The LAN Interface OK and LAN OK bits in the LAN Interface Status Word remain off.
4. A PLC fault with text "LAN system-software fault; resuming" occurs.
5. A System log event (Event 2, entry 2 = 0401H) occurs in the Station Manager event log.
6. The following “incompatible hardware” message is printed to the Station Manager display from the NODE and STAT L commands:

   This firmware version requires IC693CMM321-F or later hardware. Your hardware version is incompatible, and the network interface is unable to go online. To recover, use the firmware loader to reload firmware version 2.20. It is available from the PLC Technical Support web page. See the *TCP/IP Ethernet Communications User's Manual,* GFK-1541 for details.

To restore correct operation, update the module firmware to version 2.20. If you do not have the version 2.20 field upgrade kit, part number 44A737842-G05, download the file cmm321-r220.zip from the PLC Technical Support web page, unzip the file, and then follow the instructions in cmm321update.doc (included in the ZIP file).

System Requirements

This version of Ethernet Interface firmware requires Series 90-30 CPU firmware version 6.50 or later for full operation. Restricted operation is available with CPU firmware version 5.03 or later (6.03 for the Model 351 CPU). However, Ethernet Interface users are strongly urged to update their CPU firmware. See “Additional Restrictions with CPU Firmware Earlier than Version 6.50” on page 3.

Connecting to PLC programming software via Ethernet requires both IC693 CPU version 6.50 (or later version) and Ethernet Interface version 1.10 or higher.

Power Supply Requirements

- The Ethernet Interface requires PLC Power Supply IC693PWR321 (Rev. K or later), IC693PWR322, or IC693PWR330.
- Power consumption of the Ethernet Interface module is 700mA @ +5VDC

Configuration Through Serial Port Required Before Using Ethernet Communications

The Ethernet Interface cannot operate on the network until a valid IP address is configured. The necessary Ethernet addressing information must be configured prior to actual network operation. Two methods are available:

1. Perform the initial configuration using a PLC Programmer through the PLC CPU serial port.
2. Connect a serial terminal to the Station Manager port (port 1) of the Ethernet Interface module. Then use the CHSOSW command to enter a temporary IP address. The interface can then be reached by a PLC programmer via Ethernet. See *TCP/IP Ethernet Communications for the PLC Station Manager Manual* for details.

Proper IP Addressing is Always Essential

The Ethernet Interface must be configured with the correct IP Address for proper operation in a TCP/IP Ethernet network. Use of incorrect IP addresses can disrupt network operation. Refer to *TCP/IP Ethernet Communications User's Manual* for important information on IP addressing.

No HHP Support

The Hand Held Programmer (IC693PRG300) may ***not*** be used to configure the Ethernet Interface. Do not attempt to configure the Ethernet Interface or to read its configuration with the HHP. Such attempts may result in erroneous Loss-of-Module faults in the PLC Fault Table or other unexpected behavior.

Serial Load/Store of Register Table Causes Ethernet Programmers to Lose Communication

A load or store of the PLC Register (%R) table by a PLC Programmer connected through the CPU serial port can cause Ethernet applications that use the PLC programmer communication window to lose communication. This condition occurs when the load/store operation requires more than 10 seconds to complete. For example, transferring the %R table of a CPU341, CPU35x, CPU36x or CPU37x at 19,200 baud or less will cause the timeout. The Ethernet Interface posts two or more PLC faults with the text "LAN system-software fault; resuming", and fault-specific data starting with 080008 and/or 080042. In addition, faults with text "Bad remote application request; discarded request" (1B0021) and "Local request to send rejected; discarded request" (110005) may occur. The STAT LED on the Ethernet Interface goes out.

Logicmaster 90-30 TCP/IP Software Briefly Loses Communication When Configuration Cleared or Stored

Clearing or storing the PLC configuration causes the MS-DOS Ethernet programming software to display a flashing "NO COMMUNICATIONS" message for one or two seconds. PLC faults similar to those listed under "Serial Load/Store of Register Table Causes Ethernet Programmers to Lose Communication" above occur; the STAT LED on the Ethernet Interface goes out. In some cases, a 10 second delay occurs before loss of communication is detected.

When the PLC configuration is stored from the MS-DOS Ethernet programming software, the communications loss occurs immediately after successful completion of the store. Attempts to store configuration plus logic and/or reference tables in one operation can fail. However, storing configuration separately from logic or reference tables will always succeed.

See "Restrictions and Open Problems" on page 3 for a description of operational behavior when configuration is cleared or stored using VersaPro.

Clearing Slot Configuration Closes TCP Connections

When the PLC CPU contains version 6.50 or later firmware, clearing the slot configuration of the Ethernet Interface causes the interface to close all of its TCP connections immediately. The Ethernet Interface slot configuration is cleared when a PLC Programmer connected via Ethernet clears the PLC configuration, or stores a new configuration with an empty slot or different module type at the location where the interface is installed. PLC faults similar to those listed under "Serial Load/Store of Register Table Causes Ethernet Programmers to Lose Communication" above occur; the STAT LED on the Ethernet Interface goes out.

Applications that use the Ethernet Interface's SRTP server, such as Host Communications Toolkit client applications, must be aware that the connection has closed and take action to establish a new connection.

Extra Channels Data Transfer Entering STOP/IOSCAN Mode

Use caution when configuring the PLC CPU to scan I/O in STOP mode. There is a small time delay between a RUN to STOP/IOSCAN mode transition in the PLC CPU and the time when the Ethernet Interface deactivates repeating channels. The length of this delay varies with the PLC hardware configuration and the application program. In some cases, the time delay will be long enough that one data transfer by a repeating channel will occur after the CPU mode transition.

After a RUN to STOP/NO IO mode transition, the Ethernet Interface aborts repeating channels immediately.

RUN Mode Program Store

A store of a folder containing large (greater than 14K bytes) program blocks using a PLC Programmer via Ethernet may fail and result in momentary loss of communication. This condition has been observed only when attempting to store a large program to a PLC which is in RUN mode, and which is configured to use a limited communication window. These conditions cause the store operation to take the maximum possible period to complete. The failure may occur if this period exceeds 10 seconds for an individual program block. If this problem does occur, one of the following options may be used to complete the store operation successfully:

1. Change the PLC configuration to use Run-to-Completion mode instead of a Limited Communication Window for the store operation.
2. Change the PLC from RUN to STOP mode to complete the store.
3. Structure the folder being stored to eliminate large program blocks or subroutine blocks. This will minimize the chance that any single block will take longer than the maximum 10-second period allowed for storage of that block.

Changes and Additions to User's Manuals

TCP/IP Ethernet Communications User's Manual

The following changes will be made in Version C of the *TCP/IP Ethernet Communications User's Manual,* GFK-1541B at its next revision.

Chapter 4, "Minor Error Codes for Major Error Codes 90H (Client API Error)"

The description of Error Status 8890H should read "Invalid channel number or channel is in an inactive state (for example, the remote device has been turned off or disconnected, or the 'killms' Station Manager command was used at the remote device to stop the channel)".

Chapter 5, "Exchange Status Word Error Codes"

The following error codes should be added:

5	C	Stale data sample	The producer has indicated that the data sent was stale (data has not been updated) at the time it was produced. The exchange is used.
14	C	Data size mismatch error	The data size of a consumed exchange does not match the exchange definition. The exchange is ignored.
30	C	Major signature mismatch	Producer and consumer signatures are different, indicating a mismatched configuration. The exchange is ignored.

Chapter 6, "TCP Port Numbers" (new section, follows "MAC Addresses" section)

The TCP port number on which the SRTP server listens for incoming messages is 18245 (decimal).

The TCP port number on which the Modbus/TCP server listens for incoming messages is 502 (decimal).

Appendix E, Table E-1 "Modbus Register/IC693CMM321 Reference Table Translation"

Note that current Series 90-30 PLCs support 2048 bits of %I and %Q. The mapping table shows 4096 bits, for potential future growth. Do not attempt to read %I or %Q bits beyond 2048.

Station Manager Manual

The following will be added to the *TCP/IP Ethernet Communications for the Series 90 PLC Station Manager Manual,* GFK-1186G at its next revision.

In Table B-2, Exception Log Event Codes for Style A Station Manager, add the following:

Log Event Code	Possible Cause and Resolution
Event "2" System Events	This event is logged by the system when a catastrophic system event occurs. **Entry 2** (hexadecimal) codes are as follows: System Error: 05 "LAN system-software fault; resuming" During a field upgrade to a new software revision, an apparent hardware failure has caused repeated attempts to erase or re-program flash memory to fail. The Ethernet module may be completely inoperative after it is powered off or restarted. If so, it must be replaced.
Event "11"	The additional value 12H for Entry 2 is possible. It indicates an internal system software error that should be reported to the manufacturer.

Tally Descriptions (Appendix C)

In Table C-6 "ICMP Tallies", the tally "Filtered" should be described as:

Filtered	Number of ICMP messages ignored because they are not directly addressed to this node, or because this node has detected an invalid source address for an incoming IP or ICMP message.

Installation in Hazardous Locations

The following information is for products bearing the UL marking for Hazardous Locations:

- WARNING - EXPLOSION HAZARD - SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2;
- WARNING - EXPLOSION HAZARD - WHEN IN HAZARDOUS LOCATIONS, TURN OFF POWER BEFORE REPLACING OR WIRING MODULES; AND
- WARNING - EXPLOSION HAZARD - DO NOT CONNECT OR DISCONNECT EQUIPMENT UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NONHAZARDOUS.
- EQUIPMENT LABELED WITH REFERENCE TO CLASS I, GROUPS A, B, C & D, DIV. 2 HAZARDOUS LOCATIONS IS SUITABLE FOR USE IN CLASS I, DIVISION 2, GROUPS A, B, C, D OR NON-HAZARDOUS LOCATIONS ONLY.